IN THE SPECIFICATION

Please amend the specification as follows:

The following is inserted on page 1 at line 1, immediately following the Title, wherein the phrase "Field" is intended to retain an underline after the amendment is added to the specification:

Field

The disclosure relates to the field of broadcast applications, and more particularly to conditional access systems.

The paragraph beginning at page 1, line 1 is amended as follows:

~~The invention relates to a method for operating a conditional access system for broadcast applications, said conditional access system comprising a number of subscribers, each subscriber having a terminal including a conditional access module and a secure device for storing entitlements, wherein a source signal is encrypted using a first key (C_W), said first key (C_W) being changed at a high rate, said encrypted source signal being broadcasted for receipt by the terminals, wherein entitlement control messages (ECM's) are sent to the secure devices, said ECM's comprising the first keys (C_W) encrypted using a service key (P_I) , wherein entitlement management messages (EMM's) are sent to the secure device providing the service key (P_I) required to decrypt encrypted first keys (C_W), wherein a cracked secure device which is used in an unauthorised manner is traced by sending different keys required to obtain the first keys to different terminals or groups of terminals and monitoring the key information provided by a pirate.~~

The following is inserted on page 1 between lines 18 and 19, wherein the phrase "Background" is intended to retain an underline after the amendment is added to the specification:

Background

The following is inserted on page 2 between lines 21 and 22, wherein the phrase "Summary" is intended to retain an underline after the amendment is added to the specification:

Summary

The disclosure relates to a method for operating a conditional access system for broadcast applications, said conditional access system comprising a number of subscribers, each subscriber having a terminal including a conditional access module and a secure device for storing entitlements, wherein a source signal is encrypted using a first key (C_W), said first key (C_W) being changed at a high rate, said encrypted source signal being broadcasted for receipt by the terminals, wherein entitlement control messages (ECM's) are sent to the secure devices, said ECM's comprising the first keys (C_W) encrypted using a service key (P_T), wherein entitlement management messages (EMM's) are sent to the secure device providing the service key (P_T) required to decrypt encrypted first keys (C_W), wherein a cracked secure device which is used in an unauthorised manner is traced by sending different keys required to obtain the first keys to different terminals or groups of terminals and monitoring the key information provided by a pirate.

The following is inserted on page 4 between lines 17 and 18, wherein the phrase "Brief Description of the Drawings" is intended to retain an underline after the amendment is added to the specification:

Brief Description of the Drawings

The following is inserted on page 4 between lines 26 and 27, wherein the phrase "Detailed Description " is intended to retain an underline after the amendment is added to the specification:

Detailed Description

The paragraph beginning at page 8, line 13 is amended as follows:

> In an alternative embodiment of the method described, a cracked secure device can be traced by using a type of cryptography, wherein it is possible to generate a set of keys, each key being capable of decrypting the same cryptogram. As an example of such type of cryptography an RSA multiple-key cryptographic algorithm or a secret-sharing algorithm can be used. As the cryptography as such is not a part of the present disclosure, ~~invention,~~ reference is made to the book Applied Cryptography by Bruce Schneier, in particular chapter 23, for a further explanation of this type of cryptography. For example the [[EMM's]] EMC's are encrypted using a multiple-key algorithm having a set of keys Pi capable of decrypting the [[EMM]] EMC. Depending on the

number of keys of the set and the number of terminals, each terminal or each group of terminals is provided with a different key Pi, so that if a pirate rebroadcasts the key, the source, i.e. the cracked secure device, can be traced. It is also possible to apply this special type of cryptography on the source signal, so that in stead of one control word Cw set of control words Ci is capable of decrypting the encrypted source signal.